


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: The ACM Digital Library The Guide



Searching within **The ACM Digital Library** for: certified email for recipient ([start a new search](#))

Found 114 of 267,145

REFINE YOUR SEARCH

Refine by Keywords

Refine by People
[Names](#)
[Institutions](#)
[Authors](#)
[Editors](#)
[Reviewers](#)

Refine by Publications
[Publication Year](#)
[Publication Names](#)
[ACM Publications](#)
[All Publications](#)
[Content Formats](#)
[Publishers](#)

Refine by Conferences
[Sponsors](#)
[Events](#)
[Proceeding Series](#)

ADVANCED SEARCH

[Advanced Search](#)

FEEDBACK

[Please provide us with feedback](#)

Found 114 of 267,145

Search Results

Related Journals

Related Magazines

Related SIGs

Related C

Results 1 - 20 of 114

Sort by

Result page:

1 Multiparty nonrepudiation: A survey

Jose A. Onieva, Jianying Zhou, Javier Lopez

December 2008 **Computing Surveys (CSUR)**, Volume 41 Issue 1

Publisher: ACM

Full text available: Pdf (394.42 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [... more](#)

Bibliometrics: Downloads (6 Weeks): 50, Downloads (12 Months): 647, Downloads (Overall): 647

Nonrepudiation is a security service that plays an important role in many Internet applications. Nonrepudiation has been studied intensively in the literature. This survey focuses on multiparty nonrepudiation ...

Keywords: Multiparty applications, multiparty protocols, nonrepudiation

2 Certified mailing lists

Hrimanshu Khurana, Hyung-Seok Han

March 2006 **ASI ACCS '06: Proceedings of the 2006 ACM Symposium on Information, communication and security**

Publisher: ACM

Full text available: Pdf (431.56 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [... more](#)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 39, Downloads (Overall): 328, Downloads (Unique): 100

Email List Services (or simply, *mailing lists*) are becoming increasingly common for collecting and managing email. They enable their use for official purposes with increased effectiveness and security, services such as mailing lists ...

Keywords: certified delivery, mailing lists

3 Communications of the ACM: Volume 51 Issue 12

December 2008 **Communications of the ACM**

Publisher: ACM

Full text available: Digital Edition, Pdf (6.91 MB) Additional Information: [full citation](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 643, Downloads (12 Months): 4198, Downloads (Overall): 4198

4 interactions: Volume 15 Issue 5

September 2008 **interactions**

Publisher: ACM

Full text available:  Digital Edition ,  Pdf (13.85 MB) Additional Information: [full citation](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 95, Downloads (12 Months): 167, Downloads (Overall): 3·

5 Usable secure mailing lists with untrusted servers

 Rakesh Bobba, Joe Muggli, Meenal Pant, Jim Basney, Himanshu Khurana
April 2009 **IDtrust '09: Proceedings of the 8th Symposium on Identity and Trust on the Web**

Publisher: ACM 

Full text available:  Pdf (885.68 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 97, Downloads (Overall): 97,

Mailing lists are a natural technology for supporting messaging in multi-party, cross-domain environments. However, whenever sensitive information is exchanged on such lists, security becomes an issue. We have developed a prototype secure ...

Keywords: e-mail list security, proxy re-encryption, usability study

6 PBES: a policy based encryption system with application to data sharing in the power grid

 Rakesh Bobba, Himanshu Khurana, Musab Alturki, Farhana Ashraf
March 2009 **ASI ACCS '09: Proceedings of the 4th International Symposium on Information and Communications Security**

Publisher: ACM 

Full text available:  Pdf (1.14 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 33, Downloads (12 Months): 105, Downloads (Overall): 105,

In distributed systems users need the ability to share sensitive content with multiple other parties while maintaining privacy. This requires the ability to satisfy arbitrary policies. One such system is electricity grids where finegrained access control is required. We have developed a policy based encryption system ...

Keywords: multi-party data sharing, phasor measurement units (PMUs), policy based encryption

7 Johnny 2: a user test of key continuity management with S/MIME and Outlook Express

 Simson L. Garfinkel, Robert C. Miller
July 2005 **SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security**

Publisher: ACM

Full text available:  Pdf (665.63 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 137, Downloads (Overall): 67,

Secure email has struggled with significant obstacles to adoption, among them the low adoption rate of public key infrastructure and the cost and overhead of obtaining public key certificates. Key continuity management is a way to lower ...

Keywords: Usability, e-commerce, user interaction design, user studies

8 Certified email with a light on-line trusted third party: design and implementation

 Martín Abadi, Neal Glew
May 2002 **WWW '02: Proceedings of the 11th international conference on World Wide Web**

Publisher: ACM

Full text available:  Pdf (189.19 KB)

Additional Information: [full citation](#), [abstract](#), [cited by](#), [index](#)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 37, Downloads (Overall): 794,

This paper presents a new protocol for certified email. The protocol aims to combine security implementation, and viable deployment. The protocol relies on a light on-line trusted third party without any special ...

9 Securing the drop-box architecture for assisted living

 Michael J. May, Wook Shin, Carl A. Gunter, Insup Lee

November 2006 **FMSME '06: Proceedings of the fourth ACM workshop on Formal methods in medical systems engineering**
Publisher: ACM

Full text available:  Pdf (490.78 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 51, Downloads (Overall): 310,

Home medical devices enable individuals to monitor some of their own health information such as blood pressure or trips to medical facilities. This enables more continuous information to be provided to better ...

Keywords: assisted living, formal methods, formal verification, home health monitoring, medical devices

10 Accountability protocols: Formalized and verified

 Giampaolo Bella, Lawrence C. Paulson

May 2006 **Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1

Publisher: ACM 

Full text available:  Pdf (433.82 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 84, Downloads (Overall): 568

Classical security protocols aim to achieve authentication and confidentiality under the assumption that all parties behave honestly. Some recent protocols are required to achieve their goals even if the parties do not behave ...

Keywords: Isabelle, Nonrepudiation, certified email, inductive method, proof tools

11 Experiences in building and operating ePOST, a reliable peer-to-peer application

 Alan Mislove, Ansley Post, Andreas Haeberlen, Peter Druschel

April 2006 **EuroSys '06: Proceedings of the 1st ACM SIGOPS/EuroSys European Conference**, April 2006

Publisher: ACM

Full text available:  Pdf (382.48 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 66, Downloads (Overall): 288

Peer-to-peer (p2p) technology can potentially be used to build highly reliable applications. However, most of the existing applications, such as file sharing or web caching, have significant demands. Without ...

Keywords: decentralized systems, electronic mail, peer-to-peer, reliability

Also published in:

October 2006 **SIGOPS Operating Systems Review** Volume 40 Issue 4

12 Authenticated names

 Stanley Chow, Christophe Gustave, Dmitri Vinokurov

July 2008 **NSPW '07: Proceedings of the 2007 Workshop on New Security Paradigms**

Publisher: ACM 

Full text available:  Pdf (415.57 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 11, Downloads (Overall): 11,

Currently, most means of communication include some form of identification of the senders. These identifications are securely authenticated (at least not conveniently or in wide use). Legitimate users can be misrepresented ...

Keywords: VoIP, authentication, email, identity, instant messages, phishing, telephony

13 Verifiable encryption of digital signatures and applications

 Giuseppe Ateniese

February 2004 **Transactions on Information and System Security (TISSEC)**, Volume 7

Publisher: ACM 

Full text available:  Pdf (258.12 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 29, Downloads (12 Months): 171, Downloads (Overall): 291

This paper presents a new simple schemes for verifiable encryption of digital signatures. The party (TPP) does not take part in the protocol only if it crashes. ...

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, cryptography

14 Escrow services and incentives in peer-to-peer networks

 Bill Horne, Benny Pinkas, Tomas Sander

October 2001 **EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce**

Publisher: ACM 

Full text available:  Pdf (265.69 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 75, Downloads (Overall): 703, Downloads (Latest 12 Months): 10

Distribution of content, such as music, remains one of the main drivers of P2P development. Peer-to-peer services are currently receiving a lot of attention from the content industry as a viable distribution. One ...

15 Fair certified e-mail delivery

 Aleksandra Nenadić, Ning Zhang, Stephen Barton

March 2004 **SAC '04: Proceedings of the 2004 ACM symposium on Applied computing**

Publisher: ACM 

Full text available:  Pdf (179.18 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 53, Downloads (Overall): 709

Communication by e-mail has become a vital part of everyday business and has replaced ways of communicating. Important business correspondence may require certified e-mail provided by conventional ...

16 An intruder model for verifying liveness in security protocols

 Jan Cederquist, Mohammad Torabi Dashti

November 2006 **FMSE '06**: Proceedings of the fourth ACM workshop on Formal methods in

Publisher: ACM

Full text available:  Pdf (231.15 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [...](#)

Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 35, Downloads (Overall): 277,

We present a process algebraic intruder model for verifying a class of liveness properties. In this class, the proposed intruder model is proved to be equivalent to a Dolev-Yao intruder till the delivery ...

Keywords: Dolev-Yao intruder, intruder models, liveness properties, security protocols

17 A new fair non-repudiation protocol for secure negotiation and contract signing

 A. Ruiz-Martínez, C. I. Marín-López, L. Baño-López, A. F. Gómez Skarmeta

October 2006 **PST '06**: Proceedings of the 2006 International Conference on Privacy, Security and Trust Between PST Technologies and Business Services

Publisher: ACM 

Full text available:  Pdf (280.60 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [...](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 51, Downloads (Overall): 51,

In some scenarios, such as B2B or IPR contracting, or by legal requirement, the participation in the contract signing is required in many cases, that is, an on-line TTP. This e-notary gives the parties involved in the contract signing a guarantee that each party performs some tasks ...

Keywords: abuse freeness, confidentiality, contract negotiation, contract signing protocols, digital signatures, e-commerce, security

18 An abuse-free fair contract signing protocol based on the RSA signature

 Guolin Wang

May 2005 **WWW '05**: Proceedings of the 14th international conference on World Wide Web

Publisher: ACM

Full text available:  Pdf (198.83 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [...](#)

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 54, Downloads (Overall): 330,

A fair contract signing protocol allows two potentially mistrusted parties to exchange their digital signatures (RSA) without revealing them to each other. It allows each party to verify the other's signature (RSA) to an agreed contract over the Internet in a fair way, so that either each of the parties can verify the other's signature, or ...

Keywords: RSA, contract signing, cryptographic protocols, digital signatures, e-commerce, security

19 Fair exchange in E-commerce

 Indrajit Ray, Indrakshi Ray

March 2002 **SI Gecom Exchanges**, Volume 3 Issue 2

Publisher: ACM

Full text available:  Pdf (45.89 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 74, Downloads (Overall): 94

Many business transactions over the Internet involve the exchange of digital products such as emails, digital audio and video, electronic contract signing and digital signatures, to name a few. These transactions occur between ...

Keywords: electronic commerce, fair-exchange, protocols, security

20 Communications of the ACM: Volume 52 Issue 10

 October 2009 Communications of the ACM

Publisher: ACM

Full text available:  Digital Edition ,  Pdf (7.38 MB) Additional Information: [full citation](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 1607, Downloads (12 Months): 1607, Downloads (Overall): 1607

[Result page:](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2009 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real Player